Computer Software & Applications for Communications, Preparedness, and Security

Michael Chesbro

April 2026

This is a list of software and applications that the author has found useful for communications, preparedness, and security. The focus is on free and open-source software that can be used off-line; although the list includes other programs that may be particularly useful or interesting.

While the author has used most everything listed here, he is not the author / developer of any of these programs. If you find something useful on this list, please support the authors and developers of those programs.

7 Zip (https://7-zip.org/) is a free and open-source file archiver developed by Igor Pavlov that allows users to compress and decompress files into smaller archives or extract them from existing ones. First released on January 2, 1999, it is known for its high compression ratio, particularly with its native .7z format, which often achieves 30–70% better compression than standard ZIP files. Offers password protection and can encrypt filenames.

ADS-B Exchange

(https://www.adsbexchange.com/open-source-software/) is the world's largest source of unfiltered, uncensored flight data, founded in 2016 by Dan Streufert to provide a transparent window into global aerial movements. Unlike commercial trackers that redact certain aircraft, the platform aggregates real-time signals from a global network of enthusiast-hosted receivers to display all visible flights without censorship. Since early 2023, the service has been owned by JETNET, an aviation intelligence firm.

AllStarLink (https://www.allstarlink.org/) is a network of Amateur Radio repeaters, remote base stations and hot spots accessible to each other via Voice over Internet Protocol. AllStarLink runs on a dedicated computer (including the Raspberry Pi) that you host at your home, radio site or computer center. It is based on the open-source Asterisk PBX running our app_rpt application. App_rpt makes Asterisk a powerful system capable of controlling one or more radios. It provides linking of these radio "nodes" to other systems of similar construction anywhere in the world via VoIP.

Alpine Quest (https://alpinequest.net/en) is the complete solution for all outdoor activities and sports, including hiking, running, trailing, hunting, sailing, geocaching, off-road navigation and much more.

APKPure (https://apkpure.com/) is a multi-platform app store primarily focused on Android, providing extensive app-related content.

APRSdroid (https://www.aprsdroid.org/) is an Android application for Amateur Radio operators that allows users to send and receive APRS (Automatic Packet Reporting System) data. It provides features such as real-time tracking of APRS stations, sending position reports, and viewing weather data on a map. (For iOS see the APRS FI App)

ATAK (https://tak.gov/) stands for the Android Team Awareness Kit (or Android Tactical Assault Kit for military use), a geospatial infrastructure and situational awareness application that runs on Android smartphones. Originally developed in 2010 by the Air Force Research Laboratory (AFRL) and now maintained by the Tactical Assault Kit (TAK) Product Center, it allows users to share real-time location data, maps, and sensor information to coordinate teams across military, law enforcement, and civilian emergency response sectors. (Also: https://www.civtak.org/)

ATOC (Advanced Tactical Operation Command) (https://www.atoc.io/) lets you can create and manage Situation Reports (SITREPs), track and update their status, and assign team members to each report. Team members can be added with detailed profiles, including contact information, emergency contacts, medical conditions, drug allergies, blood type, and more. A.T.O.C. also lets you maintain comprehensive asset records—whether that's safe houses, vehicles, or fully custom entries.

Avenza Maps (https://store.avenza.com/) is a mobile application for iOS and Android that enables users to download, view, and interact with offline maps using the device's built-in GPS, requiring no cellular or Wi-Fi connectivity.

Binary Eye (https://sourceforge.net/projects/binary-eye.mirror/) is a free, open-source, and ad-free barcode and QR code scanning application designed for Android devices, developed by Markus Fisch. It utilizes the ZXing library to support a wide range of formats, including QR Code, EAN, UPC, PDF417, and Data Matrix, while also offering the capability to generate barcodes directly within the app.

Bitmessage (https://wiki.bitmessage.org/index.php/Main_Page) is a P2P communications protocol used to send encrypted messages to another person or to many subscribers. It is decentralized and trustless, meaning that you need-not inherently trust any entities like root certificate authorities. It uses strong authentication which means that the sender of a message cannot be spoofed, and it aims to hide "non-content" data, like the sender and receiver of messages, from passive eavesdroppers like those running warrantless wiretapping programs.

Bitwarden (https://bitwarden.com/) is an open-source password management service used to store sensitive information, such as website credentials, passkeys, and identity data, in an end-to-end encrypted vault. It utilizes zero-knowledge encryption (AES-CBC 256-bit and PBKDF2/Argon2id), ensuring that even the company cannot access user data. Free for personal use.

BleachBit (https://www.bleachbit.org/) is a free and open-source disk space cleaner, privacy manager, and computer system optimizer designed for Windows, macOS, and Linux systems. First released on 24 December 2008, it operates by removing junk files, cache, cookies, internet history, logs, and temporary files to free up storage and protect user privacy.

Briar (https://briarproject.org/) is an open-source, decentralized peer-to-peer messaging app designed for activists, journalists, and anyone needing secure communication without relying on centralized servers. It functions with or without internet access, syncing messages directly between devices via Bluetooth, Wi-Fi, Tor, or removable storage like USB sticks.

Bridgefy (https://bridgefy.me/) is a messaging application launched in 2014 that enables users to send text messages without an internet connection or cellular data. It operates by creating a Bluetooth mesh network that relays messages between nearby devices, allowing communication up to 100 meters (330 feet) per hop, with the network extending further as messages jump through other users' phones. The app functions entirely offline once activated, requiring only an initial internet connection for setup, and is widely used during natural disasters, large events, and protests where traditional networks fail or are censored.

CHIRP (https://chirpmyradio.com/projects/chirp/wiki/Home) is a free, open-source, cross-platform software tool designed to program and manage the memory channels of amateur radios. It allows users to upload and download radio configurations, program repeaters and simplex frequencies, set CTCSS/DCS tones, and clone settings across multiple radios without manually entering data via the radio's keypad.

Citizen (https://citizen.com/) is the essential safety app for today's world, providing real-time safety alerts, live incident videos, and 24/7 emergency assistance to keep you and your loved ones safe. Stay informed about nearby crimes, natural disasters, fires, protests, and more with instant alerts directly on your phone. Whether you're at home or on the go, Citizen's location-based alerts instantly notify you of potentially dangerous situations like property crimes, vehicle pursuits, robberies, active shooter incidents, hurricanes, wildfires, and more.

Confide (https://getconfide.com/) is specifically designed for disappearing messages, it erases text forever immediately after reading, disables screenshots on mobile, and hides text line-by-line to prevent shoulder surfing. Released in 2013, the app is available on Android, iOS, Windows, and macOS.

Cop Watch (https://www.copwatch.org.au/) is a community education program and app to help improve engagement, trust and accountability between police and the community. The Cop Watch app lets you record interactions with police - safely and legally. The app has a video recording function. It can be programmed to send alerts with your location via SMS to your family and friends during an emergency situation with the police.

Cryptomator (https://cryptomator.org/) is an open-source encryption tool for secure cloud storage. Protect your privacy for free on Dropbox, Google Drive, OneDrive, and more. It uses AES-256 encryption to protect both file content and filenames, ensuring a zero-knowledge architecture where even the cloud provider cannot access your data.

CryptPad (https://cryptpad.org/) provides a full-fledged office suite with all the tools necessary for productive collaboration. Applications include: Rich Text, Spreadsheets, Code/Markdown, Kanban, Slides, Whiteboard and Forms. All data on CryptPad is encrypted in the browser. This means no readable data leaves the user's device. Even the service administrators cannot see the content of documents or user data.

Cures A-Z (https://curesaz.com/home/) is a free smartphone app and medical guide for people who prefer to use natural therapies to manage health issues when they can, but are content to use prescription therapies when they're the better choice.

Dangerzone (https://dangerzone.rocks/) is a free and open-source project, maintained by Freedom of the Press Foundation (FPF) that destroys malware by rendering your document into pixels in a secure sandbox and reconstructing it locally as a PDF.

Defense Language Institute Foreign Language Center (DLIFLC) (https://www.dliflc.edu/elearning/) offers several free online resources for language learners, including the Online Diagnostic Assessment (ODA) to evaluate reading and listening proficiency, and GLOSS (Global Language Online Support System) for targeted lessons. The eLearning Portal provides dynamic tools like Rapport (pre-deployment certificate) and HeadStart2 (100 hours of basic training in languages such as Arabic, Chinese, and Spanish).

Dire Wolf (https://github.com/wb2osz/direwolf) is a free, open-source software "soundcard" modem/TNC and APRS encoder/decoder that

allows amateur radio operators to decode and transmit APRS packets using a computer's audio interface instead of expensive dedicated hardware. It functions as a versatile replacement for traditional Terminal Node Controllers (TNCs), capable of operating stand-alone or as a virtual TNC for other applications like Xastir, UI-View32, and APRSIS32.

Disaster Alert (https://disasteralert.pdc.org/disasteralert/) available in both iOS, Android, and on the web, Disaster Alert provides a way for people and their loved ones to stay safe anytime, anywhere with instant access to 18 different types of active hazards including: drought, earthquake, flood, storm, cyclone, tsunami, volcano, landslide, wildfire, biomedical, man-made hazards and more.

Disroot (https://disroot.org/) is a free, open-source platform based in Amsterdam, Netherlands, founded in 2015 by volunteers to provide online services based on principles of freedom, privacy, federation, and decentralization. It was created to offer ethical alternatives to proprietary "walled gardens" like Google or Microsoft, ensuring that user data is not tracked, mined, or sold to advertisers.

DRYAD Generators - The DRYAD Numeral Cipher/Authentication System is a simple, paper cryptographic system used by the U.S. military for authentication and for encryption of short, numerical messages.

- Citizen Militia (https://citizenmilitem.com/?page_id=200)
- Dougsko (https://github.com/dougsko/dryad_generator)
- Kris Hetzel (https://github.com/KrisHetzel/DRYAD-Generator)
- PK1 (https://px1.link/crypto/dryad-pad/)

EasyPal (https://easypal1.software.informer.com/13.0/) is a digital SSTV program using a soundcard to encode and decode the SSTV signals. It's also a very flexible software tool for sending and receiving files other than picture files. EasyPal (developed by Erik VK4AES, who passed away in 2015) remains the most commonly used software for Digital DRM SSTV, its development has stalled with no updates since approximately 2015.

Echolink (https://echolink.org/) is a computer-based amateur radio system distributed free of charge that allows radio amateurs to communicate with other amateur radio operators using Voice over IP (VoIP) technology on the Internet for at least part of the path between them.

EmComm Tools Community (https://community.emcommtools.com/) is a customized version of Ubuntu Linux. It is designed to be packaged as a complete operating system with all the software and configuration needed to carry out off-grid communication with near-zero configuration required by the operator.

Encryption Wizard (https://gettens.online/) is a cross-platform, Java-based file and folder encryption utility developed by the U.S. Air Force Software Protection Initiative (SPI) to protect sensitive information such as FOUO, PII, CUI, and Privacy Act data. It operates as a portable program that requires no formal installation or elevated privileges, allowing it to run on Windows, Mac OS X, Linux, and Solaris systems directly from a USB drive or local folder.

ExifTool (https://exiftool.org/) is a free, open-source, and platform-independent Perl library and command-line application for reading, writing, and editing metadata in a wide variety of files. It supports numerous metadata formats including EXIF, GPS, IPTC, XMP, JFIF, GeoTIFF, ICC Profile, and manufacturer-specific notes for cameras from brands like Canon, Nikon, Sony, and GoPro.

F-Droid (https://f-droid.org/en/) is the app distribution ecosystem for Android where your user freedom comes first.

FEMA App (https://www.ready.gov/fema-app) allows you to receive real-time weather alerts, locate emergency shelters in your area, prepare for common hazards, and more.

FidoNet (or Fido) (https://www.fidonet.org/) is a worldwide, non-commercial computer network originally founded in 1984 by Tom Jennings to connect Bulletin Board Systems (BBSes) using modems and proprietary protocols. While it peaked in the early 1990s, the network still exists today with approximately 2,000 active nodes globally, though its size has shrunk considerably compared to its historical peak. The network operates as a store-and-forward system where messages and files are exchanged between hobbyist system operators (sysops) via IP, modems, or internet gateways. The network is now largely sustained by retro-computing enthusiasts and remains particularly popular in Russia and former USSR republics.

FLDigi (https://sourceforge.net/projects/fldigi/) (short for Fast Light Digital) is a free and open-source computer program that turns a standard

sound card into a two-way data modem for amateur radio operators. It enables users to transmit and receive digital signals like PSK31, RTTY, CW (Morse code), MFSK, and Olivia by connecting a radio transceiver's microphone and headphone jacks to the computer's audio inputs and outputs. The software supports a vast array of digital modes and operating systems, including Windows, macOS, Linux, FreeBSD, and Android, and is capable of handling tasks ranging from simple keyboard-to-keyboard communication to complex emergency messaging and file transfers.

FreeDV (https://freedv.org/) is an open-source suite of digital voice modes designed specifically for HF amateur radio that allows any standard SSB radio to transmit and receive high-quality digital voice without requiring new hardware. Developed by an international team of radio amateurs and led by David Rowe (VK5DGR), the project utilizes the Codec2 speech codec to compress audio into a narrow 1.25 kHz bandwidth signal, enabling clear voice communication over the ionosphere using existing SSB equipment.

Gaggle Mail (https://gaggle.email/) is a modern email management platform designed to simplify group communication. It serves as a replacement for traditional Listservs, allowing users to create and manage mailing lists easily. Key features include a shared email address for group communication, reliable email delivery, and an intuitive interface that requires zero maintenance. This makes it an effective tool for managing group discussions and ensuring important messages reach the right audience.

GeoDa (https://geodacenter.github.io/) is a collection of software tools designed to implement techniques for exploratory spatial data analysis on

lattice data. It is intended to provide a user-friendly and graphical interface to methods of descriptive spatial data analysis, such as autocorrelation statistics and indicators of spatial outliers. Available for Windows, Mac and Unix operating systems.

GNU Privacy Assistant
(https://www.gnupg.org/related_software/gpa/) is a graphical user interface for the GnuPG (GNU Privacy Guard).

Go Anywhere OpenPGP Studio
(https://www.goanywhere.com/products/open-pgp-studio/download) is a free PGP file encryption tool that makes it easy to protect your sensitive files while complying with the Open PGP standard. It uses a safer dual-key (asymmetric) system to encrypt and decrypt information. Open PGP Studio lets you: Encrypt and decrypt files using OpenPGP, Create and verify digital signatures, Import, export, and manage encryption keys.

Google Earth (https://earth.google.com/) is a web and computer program created by Google that renders a 3D representation of Earth based primarily on satellite imagery. The program maps the Earth by superimposing satellite images, aerial photography, and GIS data onto a 3D globe, allowing users to see cities and landscapes from various angles.

Gpg4win [GNU Privacy Guard for Windows]
(https://www.gpg4win.org/) is a free, open-source encryption software suite designed for Microsoft Windows that enables users to securely encrypt and sign emails and files using OpenPGP and S/MIME standards. Originally initiated and funded by Germany's Federal Office for

Information Security (BSI), it serves as the official GnuPG distribution for Windows and is maintained by the developers of GnuPG. Gpg4win version 5.0.2 was released on 2026-03-16.

Grocy (https://grocy.info/) is a web-based, self-hosted household management solution designed to track groceries, manage pantry inventory, plan meals, and organize household chores.

Gutenberg Project (https://www.gutenberg.org/) is the oldest digital library and a volunteer effort to digitize and archive cultural works, founded in December 1971 by Michael S. Hart at the University of Illinois. Its primary mission is to encourage the creation and distribution of eBooks by making public domain works freely available to the world in open formats like plain text, HTML, EPUB, and MOBI. As of March 2026, the collection contains over 78,000 items, including novels, poetry, short stories, cookbooks, and reference works, with most releases in English but significant numbers in many other languages.

Ham Dash (https://hamdash.com/) is a free, privacy-first ham radio dashboard that puts real-time DX spots, space weather, propagation predictions, and a full operator toolkit on one screen — no account required, no tracking, no personal data stored, just open and operate.

Hams Over IP (https://hamsoverip.com/) The modern, community-driven platform of VoIP that allows ham operators to connect, communicate, and collaborate worldwide.

Hyphanet [aka Freenet] (https://www.hyphanet.org/) is peer-to-peer network for censorship-resistant and privacy-respecting publishing and communication. It is free software which lets you anonymously share files, browse and publish "freesites" (web sites accessible only through Hyphanet) and chat on forums, without fear of censorship. Hyphanet is decentralized to make it less vulnerable to attack, and if used in "darknet" mode, where users only connect to their friends, is very difficult to detect.

I2P (Invisible Internet Project) (https://i2p.net/en/) is a decentralized, privacy-focused network that allows people to communicate and share information anonymously. It works by routing data through multiple encrypted layers across volunteer-operated nodes, hiding both the sender's and receiver's locations. The result is a secure, censorship-resistant network designed for private websites, messaging, and data sharing.

InaSAFE (https://github.com/inasafe/inasafe) is a free, open-source QGIS plugin developed to estimate the realistic impact of natural disasters, such as floods, earthquakes, and volcanic eruptions, on communities, infrastructure, and the environment.

Internet in a Box (https://internet-in-a-box.org/) is a low-cost, open-source offline digital library that creates a local Wi-Fi hotspot, allowing multiple nearby devices to access pre-loaded educational and informational content without an active internet connection. Typically built on Raspberry Pi hardware, the system serves a vast collection of resources including Wikipedia (in multiple languages), Khan Academy Lite, OpenStreetMap, Moodle, and thousands of e-books and instructional videos.

Internet Relay Chat (IRC) is an internet protocol that lets you communicate with people with text in real-time. While IRC has been declining in popularity in favor of other chat systems like Discord and Telegram, it is still widely used amongst tech enthusiasts and the open-source software community. **W3C** (https://webirc.w3.org) allows you to access IRC from their webpage. **ClicksAndWhistles** (https://clicksandwhistles.com/) is a free IRC client for Windows. **IRCCloud** (https://www.irccloud.com/) is a free IRC client for Android and iOS.

Internxt (https://send.internxt.com/) Files uploaded and sent through Internxt Send use Internxt's disruptive zero-knowledge architecture to maximize the security and privacy of files. All files and photos are end-to-end encrypted, meaning all your information is secure before ever leaving your device. Internxt also offers 1GB of encrypted cloud storage for free.

InterPlanetary File System (IPFS) (https://ipfs.tech/) is a decentralized, peer-to-peer protocol for distributed file storage and sharing that replaces traditional location-based addressing with content-based addressing, allowing files to be uniquely identified by their cryptographic hash (CID) rather than a server IP address. Originally introduced in 2015 it enables users to host and retrieve data across a global network of nodes, making the system more resilient to censorship, permanent, and efficient compared to the centralized HTTP model.

Jami (https://jami.net/) is a free/libre, end-to-end encrypted, and private communication software. Unlike traditional messaging apps that rely on central servers to relay messages, Jami connects users peer to peer. This means each device acts as a node in a decentralized web, sending

encrypted data directly to others, without any intermediary. See more at (https://jami.net/jami-survival-kit-your-backup-solution-in-case-of-internet-failure/)

JavaScrypt: Browser-Based Cryptography Tools (https://www.fourmilab.ch/javascrypt/) is a data encryption solution which runs entirely in your web-browser. To use the page, your browser must support JavaScript and you must not have disabled execution of that language. JavaScrypt's encryption facilities use the Advanced Encryption Standard (AES).

Jitsi (https://meet.jit.si/) is a collection of free, open-source projects that enable secure video conferencing, voice over IP (VoIP), and instant messaging across web, mobile, and desktop platforms. Originally started in 2003 as "SIP Communicator" by Emil Ivov, the project evolved to focus on Jitsi Meet and Jitsi Videobridge, which power browser-based, multi-party video calls without requiring downloads or accounts. Today, Jitsi is maintained by 8x8 and operates the free public service, supporting up to 100 participants at a time.

JS8Call (https://js8call.com/) is a weak-signal, keyboard-to-keyboard messaging mode for amateur radio that combines the robustness of FT8 with a messaging and network protocol layer to enable real-time text communication and message relaying.

Kanopy (https://www.kanopy.com/) is an on-demand streaming video platform for public and academic libraries that offers films, TV shows, educational videos and documentaries. The service is free for end users,

but libraries pay fees on a pay-per-view model, from which content owners and content creators are paid.

KDE Connect (https://kdeconnect.kde.org/) is a free, open-source multi-platform application developed by KDE that enables wireless communication and data transfer between devices over a local network. It allows users to seamlessly integrate their smartphones (Android, iOS) and computers (Linux, Windows, macOS) by facilitating file sharing, clipboard synchronization, notification syncing, and remote control of media players or presentations.

KeePassXC (https://keepassxc.org/) is a free and open-source, cross-platform password manager designed for users who require high security and full control over their data without relying on cloud services.

Keybase (https://keybase.io/) is an open-source, end-to-end encrypted platform that combines secure messaging, cloud storage, and identity verification to protect user data across devices. Owned by Zoom Video Communications since May 2020, it allows users to prove ownership of social media identities (like Twitter, Reddit, and GitHub) by linking them to encryption keys in a publicly auditable manner. The platform features Keybase Chat for private communication, Keybase Filesystem (KBFS) for up to 250 GB of free encrypted cloud storage, and encrypted Git repositories for code hosting. While development has stopped following the Zoom acquisition, the service remains functional for existing users to maintain secure chats, share files, and manage team collaboration.

Kindle App (https://www.amazon.com/b?ie=UTF8&node=16571048011) is a free reading application developed by Amazon that turns smartphones, tablets, and computers into e-readers, allowing users to access millions of eBooks, magazines, comics, and audiobooks. It is available for iOS (iPhone, iPad, Mac), Android, and Windows PC.

Kiwix (https://get.kiwix.org/en/) is a free and open-source offline web browser and non-profit organization dedicated to making free educational content accessible without an internet connection. Created by Emmanuel Engelhart and Renaud Gaudin in 2007, it allows users to download and browse compressed archives of websites. The software is designed to work on computers without internet, slow connections, or in censored environments, offering features like full-text search and tabbed navigation. It supports a vast library of content including Wikimedia projects (Wikisource, Wikivoyage), Project Gutenberg texts, Stack Exchange sites, and TED talks.

Kleopatra (https://apps.kde.org/kleopatra/) is an open-source certificate manager and graphical user interface (GUI) for GnuPG (GPG), designed to simplify the management of OpenPGP and S/MIME encryption keys. It allows users to create, import, export, and manage public and private keys for encrypting and decrypting files, emails, and messages without needing to use complex command-line tools.

Libib (https://www.libib.com/) is a cloud-based library management and cataloging system designed for individuals, schools, and small organizations to organize collections of books, board games, movies, music, and video games. It functions as both a website and a mobile app

(available on iOS and Android) that allows users to scan ISBN/UPC barcodes to instantly digitize physical media, eliminating manual entry.

LibreMesh (https://libremesh.org/) is a modular, open-source framework based on OpenWrt that allows users to create auto-configurable wireless mesh networks for communities. Originally launched in 2013 by free network activists, it enables routers to automatically form decentralized networks where every node can route traffic for others, eliminating the need for a central server.

LibreOffice (https://www.libreoffice.org/) is a free, open-source office productivity suite developed by The Document Foundation, serving as a powerful alternative to Microsoft Office with no licensing fees or subscriptions. Initially released as a fork of OpenOffice.org in January 2011, it is compatible with major formats including .docx, .xlsx, and .pptx while using OpenDocument Format (ODF) as its native standard.

LibreWolf (https://librewolf.net/) is a free, open-source fork of Mozilla Firefox designed with a primary emphasis on privacy and security, developed by the LibreWolf Community. It removes telemetry, data collection, and anti-freedom features like DRM to provide a hardened browsing experience right out of the box. In 2022, LibreWolf was noted alongside **Brave** (https://brave.com/) and TOR as having the highest privacy protection among browsers, though it may not have full compatibility with every website due to its aggressive anti-tracking measures.

Local Send (https://localsend.org/) is a free, open-source, cross-platform file-sharing application that allows users to securely share files and messages directly between devices on the same local network without the need for an internet connection.

LokiNet (https://lokinet.org/) is an anonymous, decentralized, and IP-based overlay network that uses the Oxen Service Node network to route traffic, providing a low-latency onion routing protocol (LLARP) for private internet access. Unlike Tor, which operates at the transport layer, Lokinet functions at the network layer (Layer 3), allowing it to route any IP-based protocol including TCP, UDP, and ICMP, which enables real-time voice calls, video streaming, and gaming in addition to web browsing.

Mailfence (https://mailfence.com/) is a Belgian encrypted email service launched in November 2013 by the Contact Office Group, offering a comprehensive suite of privacy-focused tools including email, calendar, contacts, document storage, and groups. It is designed to protect user privacy through OpenPGP-based end-to-end encryption for content and TLS for transport, allowing users to send secure PGP emails to any provider while maintaining interoperability with standard email clients.

Mailvelope (https://mailvelope.com/en) is a free, open-source browser extension that adds end-to-end email encryption to webmail services like Gmail, Yahoo, and Outlook using the OpenPGP standard. It allows users to encrypt and sign messages (including attachments) directly within their browser without needing a separate email client.

ManyVerse (https://www.manyver.se/) is a decentralized, peer-to-peer social network designed to function off the grid, where all user data lives locally on the device rather than in a company-owned cloud. It uses the Secure Scuttlebutt (SSB) protocol to enable users to write posts, comment, and sync updates with friends via Bluetooth, local Wi-Fi, or the internet, even when offline.

Marble (https://marble.kde.org/) is a free and open-source virtual globe and world atlas developed by the KDE community, designed to help users explore the Earth, the Moon, Venus, Mars, and other planets. First released in November 2006, the application is written in C++ using the Qt framework and operates under the GNU LGPL license. It functions as a flexible educational tool that supports various map themes, including topographic, satellite, street, and historical maps, and can be integrated into other programs as a widget.

Mastodon (https://joinmastodon.org/) is a free, open-source, decentralized social networking platform designed as an alternative to centralized services like X (formerly Twitter). Launched in 2016, it operates as a federated network of independent servers called instances, where users can post short-form messages known as "toots," share media, and engage in discussions without a single governing company.

Medical Support to Irregular Warfare - GPT
(https://prolongedfieldcare.org/2025/11/23/introducing-mars-the-medical-advisor-for-resistance-support-gpt-a-strategic-enabler-for-medical-resistance-resilience-and-readiness/) In the face of rising global instability, authoritarian resurgence, and hybrid warfare threats, resistance movements and irregular warfare practitioners face profound challenges—

not only in confronting oppression, but in doing so while sustaining their people, preserving legitimacy, and withstanding long-term attrition. One of the most fragile elements in any resistance effort is medical support—and it is often the most targeted by hostile regimes. To help address this critical gap, we've developed the "Medical Support to Irregular Warfare" GPT—a customized AI advisor built specifically to support practitioners of irregular warfare, civil resistance organizers, medical planners, and defense policymakers operating in contested, denied, or occupied environments.

MeshCore (https://meshcore.co.uk/) is a multi-platform, open-source system designed for secure, off-grid text-based communication using LoRa radio hardware, allowing devices to form a decentralized mesh network without relying on the internet or cellular networks. Introduced in early 2025 by founder Andy Kirby, it functions as a lightweight C++ library enabling multi-hop packet routing where messages are relayed between nodes to extend range and ensure delivery.

Meshtastic (https://meshtastic.org/) is a community-driven, open-source project that transforms inexpensive LoRa radios and microcontrollers into a decentralized, off-grid mesh network for long-range, low-power messaging. It operates on unlicensed ISM radio bands, allowing users to exchange text messages, GPS locations, and sensor data without relying on cellular networks, Wi-Fi, or the internet.

MMSSTV (https://hamsoft.ca/pages/mmsstv.php) is a program developed by JE3HHT- Makoto Mori for amateur radio operators to transmit and receive analog SSTV signals using a PC soundcard. With this SSTV (slow scan television) utility, images can be sent and received using a

computer, a keying circuit and a ham radio on both the VHF and HF bands.

Morse Code is widely considered a critical backup for survival communications when modern infrastructure fails or voice transmission is impossible. Its low power requirements, ability to penetrate high noise levels, and versatility in using sound, light, or movement make it uniquely effective in emergencies where cell towers, Internet, and even standard voice radios may be unavailable. **W1AW** Morse Code Practice MP3 Files (https://www.arrl.org/code-practice-files) along with the **G4FON** (https://www.g4fon.net/) training software is useful for learning Morse Code. Additional resources for learning Morse Code can be found on the **ARRL** website (https://www.arrl.org/learning-morse-code).

Mullvad (https://mullvad.net/en) is a commercial VPN service based in Sweden, launched in 2009 by Amagicom AB in Göteborg. Its name means "mole" in Swedish, symbolizing stealth and privacy. Mullvad VPN allows users to mask their IP addresses, encrypt internet traffic, and prevent tracking by ISPs, governments, or third parties. It supports both WireGuard and OpenVPN protocols, offering secure and fast connections, and also provides Shadowsocks for bypassing censorship. Users can create accounts anonymously using a unique 16-digit number without providing personal information.

Mumble (https://www.mumble.info/) is a free, open source, low latency, high quality voice chat application.

Musicolet (https://krosbits.in/musicolet/) is a small yet powerful offline Music Player for Android, which organizes and plays local audio-files stored on your device.

My Pantry Tracker (https://mypantrytracker.com/) is a free app that helps you keep your pantry organized by keeping a detailed inventory. You can keep track of quantity, expiration dates, prices, and more. Automatically add items by scanning their barcodes with your device's camera! Available on iPhone and Android, as well as in your web browser.

NOAA Weather App
(https://play.google.com/store/apps/details?id=com.nstudio.weatherhere.free&hl=en_US) This app provides forecasts, animated radar, hourly forecast, and current conditions.

Onion Share (https://onionshare.org/) is a free, open-source tool that enables users to securely and anonymously share files, host websites, and chat using the Tor network without requiring any third-party servers or accounts. Created by Micah Lee and maintained by the Freedom of the Press Foundation, it operates by turning the user's computer into a temporary web server accessible only via an unguessable .onion address visible in Tor Browser.

Onxmaps (https://www.onxmaps.com/) is a private American technology company that develops digital mapping applications for outdoor recreation, founded in Missoula, Montana in 2009. The company offers a suite of GPS-based apps including onX Hunt, onX Offroad, onX Backcountry, and onX Fish, designed to provide accurate land ownership

data, topographic maps, and offline navigation for activities like hunting, hiking, off-roading, and fishing.

OpenPuff Steganography

(https://embeddedsw.net/OpenPuff_Steganography_Home.html) is a professional, free, and portable steganography tool for Microsoft Windows developed by Cosimo Oliboni, designed to hide sensitive data within common carrier files like images, audio, and video. It was first released in December 2004 and remains the first tool of its kind to allow users to split hidden data across multiple carrier files, forming a "carrier chain" with no enforced theoretical size limit other than available storage (up to 256MB or more depending on implementation).

OpenStego (https://www.openstego.com/) is a steganography application that provides two functionalities: (1) Data Hiding: It can hide any data within an image file. (2) Watermarking: Watermarking image files with an invisible signature. It can be used to detect unauthorized file copying.

Open Street Maps (https://www.openstreetmap.org/) is a free, editable, and collaborative map of the world created by a global community of volunteers rather than a single corporation. Founded in 2004 by Steve Coast in the United Kingdom in response to restrictive licensing on national map data, it operates as a massive open-source geospatial database available in 96 languages. The project allows anyone to view, edit, and download raw geographical data for any purpose, including routing, scientific mapping, gaming, and humanitarian aid, provided they adhere to the Open Database License (ODbL) and provide attribution. Unlike proprietary services like Google Maps, OSM offers full offline support, no

usage fees for the data itself, and complete flexibility for developers to build custom applications, self-host services, or combine data with other open datasets.

Organic Maps (https://organicmaps.app/) is a privacy-focused offline maps & GPS app for hiking, cycling, biking, and driving. Organic Maps supports 100% of its features without an active Internet connection.

OsmAnd (https://osmand.net/) (OpenStreetMap Automated Navigation Directions) is a free and open-source map and navigation application available for Android and iOS devices. It utilizes OpenStreetMap (OSM) data to provide offline maps and turn-by-turn routing with visual and voice guidance for driving, walking, biking, and public transport.

Paranoia Works Encryption Software (https://paranoiaworks.mobi/) is a suite of cross-platform symmetric encryption tools developed by Paranoia Works that secures text, files, and folders on iOS (iPhone/iPad), macOS, Windows, Linux, and Android using multiple strong ciphers. The suite includes Paranoia Text Encryption (for notes, SMS, emails, and crypto keys) and Paranoia File Encryption (which creates .enc archive files and can wipe originals), with steganography features to hide text within JPEG images using the F5 algorithm.

Paste Bin (https://pastebin.com/) is a website where you can store any text online for easy sharing. The website is mainly used by programmers to store pieces of sources code or configuration information, but anyone is more than welcome to paste any type of text. The idea behind the site is to make it more convenient for people to share large amounts of text online.

PeaZip (https://peazip.com/) is a free, open-source file archiver and file manager utility developed by Giorgio Tani, designed as a cross-platform alternative to proprietary software like WinZip and WinRAR. Released under the LGPLv3 license, it supports over 200 archive formats (including ZIP, 7Z, RAR, TAR, and its native PEA format) across Windows, Linux, macOS, and BSD systems.

pfPgpEncryptor
(https://www.softpedia.com/get/Security/Encrypting/pfPgpEncryptor.shtml) can encrypt and decrypt your important documents to prevent unauthorized access to their content. Relying on the OpenPGP standard, it can protect both files in your computer or plain text. The application provides support for some of the most used encryption standards (such as CAST5, Blowfish, AES (128, 192, 256), Twofish, DES, Safer or IDEA) and can make use of multiple hash and compression algorithms in order to ensure that the input document is impossible to access by those who don't know the security key.

PGP / GnuPG (https://www.openpgp.org/) (https://www.gnupg.org/) is an encryption program that provides cryptographic privacy and authentication for data communication. PGP is used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications.

Picture This (https://www.picturethisai.com/) offers a powerful plant identifier to identify flowers, leaves, trees, herbs, and more in seconds!

PinPoint APRS (https://www.pinpointaprs.com/) is free software that allows you to visually track and communicate with people using Amateur Radio ("Ham Radio") equipment. During an emergency, it can be used as a location aware tactical communications tool. It is mostly used as a tool for tracking people and assets on a map, although it is capable of so much more. During, for instance, a weather spotting event, an incident commander could visually track where spotters are deployed in the field, and direct them away from approaching weather using an area map on a computer screen.

PlantIn (https://myplantin.com/) Take a photo of any plant and get an accurate result using our extensive plant database. Identify any rare plants quickly and precisely, and make your identification simple and reliable with one of the largest collections of plant species.

PortableApps (https://portableapps.com/) is a platform and website that distributes free, open-source applications for Windows packaged for portability, allowing users to run software directly from removable storage devices like USB flash drives, cloud folders, or external drives without installation. Founded by John T. Haller in 2004 and launched as a community site in 2006, it enables users to carry their favorite apps, settings, and data with them across different computers. The PortableApps.com Platform serves as a central hub with a built-in app store, allowing users to download, organize, and automatically update over 1,400 portable packages (including nearly 500 real apps) via a custom menu. These applications run entirely from a single directory, storing user data and configuration settings locally within the app folder rather than modifying the host system's registry or system files.

Project Nomad (https://www.projectnomad.us/) is the most prominent recent iteration, a free, open-source, self-contained offline knowledge and education server developed by Crosstalk Solutions (Chris Sherwood). Designed to run on any local computer without an internet connection, it bundles local AI (via Ollama and Qdrant), offline Wikipedia (via Kiwix), educational platforms (Kolibri/Khan Academy), maps, and survival tools into a single Docker-based system. It stands for Node for Offline Media, Archives, and Data and is intended for preppers, off-grid living, and digital independence.

Privacy Virtual Card (https://app.privacy.com/join/5D9DA) is a service that you can use to make an online payment using virtual cards instead of your physical payment card information. With a separate Privacy Virtual Card for each merchant you shop with, your physical card is safe and secure. You can pause or close Privacy Cards at any time, preventing any future transactions from being authorized. Privacy Cards can also be Single-Use, meaning they close after just one authorized transaction thus preventing re-occurring charges or auto-billing. Every virtual card is connected to your bank account but comes with a unique, 16-digit card number, CVV, and expiration. Privacy directly debits your funding source for transactions as you make them.

Private Bin (https://privatebin.info/) is a minimalist, open source online pastebin where the server has zero knowledge of stored data. Private Bin is a fork of ZeroBin, originally developed by Sébastien Sauvage. Private Bin was refactored to allow easier and cleaner extensions and has many additional features.

PrivNote (https://privnote.com/) is a secure application for creating and sharing self-destructing notes.

Proton [Protonmail] (https://proton.me/) is the world's largest end-to-end encrypted email service, owned by the Swiss-based company Proton AG and launched in 2014 by scientists from CERN and MIT. It guarantees privacy through zero-access encryption, ensuring that only the sender and recipient can read messages, while the company itself cannot access or decrypt user data.

Psiphon (https://psiphon.ca/) is a free and open-source Internet censorship circumvention tool designed to help users bypass government-imposed content filtering and access the uncensored internet. Originally developed by the Citizen Lab at the University of Toronto in 2006, it is now maintained by Psiphon, Inc., a Canadian corporation that operates a network of thousands of proxy servers using VPN, SSH, and Web proxy technologies.

QGIS (https://qgis.org/) (formerly Quantum GIS) is a free, open-source geographic information system (GIS) software that enables users to create, edit, visualize, analyze, and publish geospatial data. It runs on Windows, macOS, Linux, and Android (via apps like QField) and supports a wide range of data formats, including vector, raster, point cloud, and database layers like PostGIS.

qTox (https://qtox.github.io/) is a free, open-source, encrypted instant messaging client that uses the peer-to-peer Tox protocol to provide secure text, voice, video calls, and file transfers without relying on central servers.

Rattlegram (https://hamradio.my/2025/06/rattlegram-the-sound-of-digital-messaging/) is an innovative app that allows users to send and receive text messages through sound, utilizing a method called COFDMTV (Coded Orthogonal Frequency Division Multiplexing with Time Variation). This technology encodes text into audio signals, enabling communication without the need for traditional cables or internet connections. Rattlegram is available on both iOS and Android platforms and is built on open-source software, ensuring privacy as it does not record or store audio beyond the final decoded text message.

ReadEra (https://readera.org/) reads multiple types of formats: book Epub, Kindle (MOBI, AZW3), Fb2; business PDF, Djvu; office Microsoft Word (DOC, DOCX, RTF), ODT; text TXT; comics CBR, CBZ, and others. Reading books, viewing Microsoft Word documents and PDF files from zip and rar archives.

Red Cross Emergency App (https://www.redcross.org/get-help/how-to-prepare-for-emergencies/mobile-apps.html) is a free, highly-rated tool available for iOS and Android that provides real-time NOAA severe weather alerts, hurricane tracking, and an interactive map to locate open Red Cross shelters and disaster services.

Relavint Desktop (https://www.accurint.com/relavintdesktop.html) by LexisNexis is an easy-to-use visualization and drawing tool specifically designed for creating link analysis charts—visual relationships between individuals and their relatives, associates, addresses, vehicles, corporations, and other items.

Repeater Book (https://www.repeaterbook.com/) is a worldwide, free amateur radio repeater directory and mobile app maintained by a global network of volunteer radio operators and local administrators. It serves as the most comprehensive database of its kind, allowing users to search for repeaters by location, frequency, band, or digital mode (such as DMR, P25, NXDN, and Yaesu System Fusion) without requiring an internet connection once data is loaded. The app works without a network connection, displaying distance, heading, and full repeater details based on GPS or manual search.

Reticulum (https://reticulum.network/) is a cryptography-based networking stack for building both local and wide-area networks with readily available hardware, that can continue to operate under adverse conditions, such as extremely low bandwidth and very high latency. Reticulum is a complete networking stack, and does not need IP or higher layers, although it is easy to utilize IP (with TCP or UDP) as the underlying carrier for Reticulum. It is therefore trivial to tunnel Reticulum over the Internet or private IP networks. Reticulum is built directly on cryptographic principles, allowing resilience and stable functionality in open and trustless networks. No kernel modules or drivers are required. Reticulum can run completely in userland, and will run on practically any system that runs Python 3. Reticulum runs well even on small single-board computers like the Pi Zero.

Ricochet Refresh (https://www.ricochetrefresh.net/) is an open-source, peer-to-peer instant messaging application designed for anonymous and metadata-resistant communication by utilizing the Tor network to connect users directly without central servers. Supported by the non-profit

Blueprint for Free Speech, the software ensures that no one knows your identity, your contact list, or the content of your messages, making it particularly vital for whistleblowers, activists, and journalists.

RiseupVPN (https://riseup.net/en/vpn) offers a personal VPN service for censorship circumvention, location anonymization and traffic encryption. To make this possible, it sends all your internet traffic through an encrypted connection to riseup.net, where it then goes out onto the public internet. Unlike most other VPN providers, Riseup does not log your IP address.

Robot36 (https://robot36-sstv-image-decoder.soft112.com/) is an app for both Android and iOS users that specializes in decoding and transmitting SSTV images directly on a smartphone.

RTL-SDR (https://www.rtl-sdr.com/) is a very cheap ~$30 USB dongle that can be used as a computer-based radio scanner for receiving live radio signals in your area (no internet required). Depending on the particular model it could receive frequencies from 500 kHz up to 1.75 GHz. Most software for the RTL-SDR is also community developed, and provided free of charge. Note that RTL-SDRs cannot transmit.

Safenote (https://safenote.co/) is the free, fast, and secure way to share files and notes with end-to-end encryption and a link that expires automatically. Encrypt and send files and notes with a link that automatically destruct after being read. SafeNote is a free web-based service that allows you to share a note or a file with confidentiality.

Scanner Radio
(https://play.google.com/store/apps/details?id=com.scannerradio) is a free mobile application available on iOS and Android that allows users to listen to live police, fire, weather, air traffic, and marine radio streams from over 8,000 scanners worldwide. Developed by GordonEdwards.net LLC, the app aggregates audio feeds provided by volunteers and emergency departments, primarily through the Broadcastify network, to deliver real-time breaking news and emergency updates.

SecureDrop (https://securedrop.org/) is a free and open-source software platform designed for secure communication between journalists and sources. It is an open-source whistleblower submission system that media organizations and NGOs can install to securely accept documents from anonymous sources. SecureDrop uses the anonymity network Tor to facilitate communication between whistleblowers, journalists, and news organizations, ensuring that the data is encrypted in transit and at rest. The platform is accessible as onion services in the Tor network, and it is designed to be used in high-risk environments.

SecurePost (https://apkpure.com/securepost/org.securepost.securepost) developed at UC Santa Barbara, allows dissidents to communicate anonymously on social media while verifying credibility—a response to surveillance seen during the Arab Spring. It allows a group to share a single account without sharing passwords, as every post is cryptographically signed to verify authenticity while maintaining the anonymity of individual group members.

Send (https://send.vis.ee/) is a fork of Mozilla's discontinued Firefox Send service which allows you to send files to others with a link. Files are

encrypted on your device so that they cannot be read by the server, and they can be optionally password-protected as well.

Session (https://getsession.org/) is a decentralized, open-source, end-to-end encrypted instant messaging application developed by the non-profit Session Technology Foundation, which moved its operations from Australia to Switzerland in 2024. Unlike traditional messengers, it does not require a phone number or email address for registration, instead assigning users a random 66-digit alphanumeric Account ID to ensure anonymity. Session is one of the most privacy-focused messaging apps available today.

Sideband (https://github.com/markqvist/Sideband) is a privacy-focused, peer-to-peer messaging protocol that allows users to communicate directly over local networks or the internet without servers. It emphasizes metadata resistance and secure message delivery, making it ideal for use in community networks, crisis response, and decentralized communications infrastructure. Sideband operates on the Reticulum network, supporting various mediums like LoRa, Packet Radio, and WiFi, and is completely free, end-to-end encrypted, and permission-less.

Signal (https://signal.org/) is a free, open-source, privacy-focused messaging app that provides end-to-end encryption for text messages, voice calls, and video calls. Developed by the Signal Foundation (a nonprofit) and Signal Messenger LLC, it ensures that only the sender and recipient can read messages or listen to calls, as no data is stored on the cloud and the company cannot access user communications.

SimpleX Chat (https://simplex.chat/) is the first messaging network that operates without any user identifiers (not even random numbers, phone numbers, or usernames), making it 100% private by design. Unlike other messengers, it stores all user data on client devices and uses uni-directional message queues to prevent servers from building social graphs or connecting users. Key features include quantum-resistant end-to-end encryption, secret chat groups, and the ability to connect via QR codes or one-time links without requiring email or passwords.

Syncthing (https://syncthing.net/) is a continuous file synchronization program. It synchronizes files between two or more computers in real time, safely protected from prying eyes. Your data is your data alone and you deserve to choose where it is stored, whether it is shared with some third party, and how it's transmitted over the Internet.

TAILS (https://tails.net/) (The Amnesic Incognito Live System) is a free, open-source, security-focused Debian-based Linux distribution designed to preserve privacy and anonymity against surveillance. It runs entirely from a USB stick or DVD in the computer's RAM, leaving no digital footprint on the host machine unless the user explicitly enables encrypted "Persistent Storage."

Telegram (also known as Telegram Messenger) (https://telegram.org/) is a cloud-based, cross-platform social media and instant messaging (IM) service. It launched for iOS on 14 August 2013 and Android on 20 October 2013. It allows users to exchange messages, share media and files, and hold private and group voice or video calls as well as public livestreams. It is available for Android, iOS, Windows, macOS, Linux, and web browsers. Telegram offers end-to-end encryption in voice and video calls, and

optionally in private chats if both participants use a mobile device. Telegram also has social networking features, allowing users to post stories, create public groups with up to 200,000 members, and share one-way updates to unlimited audiences in so-called channels.

TOR Project (https://www.torproject.org/) is a 501(c)(3) nonprofit organization founded on December 22, 2006, by computer scientists Roger Dingledine and Nick Mathewson to advance human rights and freedoms by creating and deploying free and open-source anonymity and privacy technologies. Its primary mission is to defend users against tracking, surveillance, and censorship by maintaining the Tor anonymity network, which bounces communications around a distributed network of volunteer-run relays to prevent observers from learning what sites a user visits or where they are located. The organization develops key tools including Tor Browser, Orbot (for Android and iOS), Tails, and Snowflake to ensure unrestricted access to an uncensored internet.

TOX Chat (https://tox.chat/index.html) Whether it's corporations or governments, digital surveillance today is widespread. Tox is easy-to-use software that connects you with friends and family without anyone else listening in. While other big-name services require you to pay for features, Tox is completely free and comes without advertising — forever.

Tuta [Tutanota] (https://tuta.com/) is a German-based, end-to-end encrypted secure email service and calendar app run by Tutao GmbH. Launched in 2011 and rebranded in November 2023, it offers a freemium model with over 10 million users as of mid-2023, prioritizing privacy by encrypting emails, contacts, and calendar entries so that even the provider cannot read the content.

Usenet is a decentralized, global discussion and article distribution system created in 1979. It operates as a worldwide network of servers that exchange messages, known as articles, across topic-based categories called newsgroups, rather than relying on a single central server. To access Usenet in 2026, you must subscribe to a premium provider, install a newsreader client, and configure SSL security. The most straightforward methods involve using an all-in-one provider like **Easynews** (https://www.easynews.com/), which offers a web-based interface with no software required, or a Tier-1 provider like **Newshosting** (https://www.newshosting.com/) or **Eweka** (https://www.eweka.nl/en), which include free newsreaders and built-in search tools.

Ushahidi (https://www.ushahidi.com/) helps communities turn information into action with an intuitive and accessible crowdsourcing and mapping tool. By enabling the rapid collection, management and analysis of crowdsourced information, Ushahidi empowers everyone—individuals, community groups, governments, activists, organizations—to create meaningful change.

VarAC (https://www.varac-hamradio.com/) (Vara Chat) is a free, modern HF P2P real-time chat application for amateur radio operators that leverages the VARA protocol to enable robust keyboard-to-keyboard communication. Developed by Irad Deutsch, 4Z1AC, it operates as a chat client sitting on top of the VARA modem software (VARA HF, FM, or SAT), allowing users to chat via HF, VHF, UHF, and satellite links with features like real-time typing indicators, file and image transfer, and emergency communication (EmComm) modes.

VeraCrypt (https://veracrypt.io/en/Home.html) is a free, open-source disk encryption utility that creates virtual encrypted disks within files and encrypts partitions or entire storage devices with pre-boot authentication. It is a fork of the discontinued TrueCrypt project, initially released on June 22, 2013, and is currently maintained by IDRIX (France) and AM Crypto (Japan).

VOACAP (https://www.voacap.com/) is free professional high-frequency (3-30 MHz) propagation prediction software from NTIA/ITS, originally developed for Voice of America (VOA).

Voxer (https://www.voxer.com/) is a free app that allows users to send and receive real-time voice messages, similar to a walkie-talkie, while also recording messages for later playback. It works on iOS, Android, and Windows devices over any cellular data network (2G, 3G, 4G, LTE) or WiFi, enabling communication anywhere in the world. Users can communicate one-on-one or in groups of up to 500 people, making it suitable for personal, professional, and team use.

What3Words (https://what3words.com/) is a proprietary geocoding system that divides the entire Earth into a grid of 57 trillion 3-by-3-meter squares, assigning each a unique, fixed combination of three dictionary words. Founded in 2013 by Chris Sheldrick, Jack Waley-Cohen, Mohan Ganesalingam, and Michael Dent, the system allows users to identify any precise location on the planet using a simple address format like *///clear.sheets.title* instead of traditional street addresses or complex GPS coordinates.

Whonix (https://www.whonix.org/) is a free, open-source Linux operating system designed specifically for advanced anonymity and privacy by routing all internet traffic through the Tor network. It operates using a unique dual-VM architecture consisting of a Whonix-Gateway (which handles Tor routing) and a Whonix-Workstation (an isolated environment for user applications), ensuring that even if the workstation is compromised, the user's real IP address remains hidden.

WikEM [The Global Emergency Medicine Wiki] (https://wikem.org/wiki/Main_Page) is the world's largest and most popular emergency medicine open-access reference resource.

WikiMed (https://meta.wikimedia.org/wiki/Wiki_Project_Med/App) offers offline access to 70,000+ medical articles, the largest collection of health-related content in English. The offline medical encyclopedia offers the largest collection of medical articles for Android, based on Wikipedia. The app contains articles on topics such as medicine, anatomy, pharmaceuticals and hygiene and gives you free access to one of the most reliable and up-to-date medical dictionaries - anywhere in the world, even without an internet connection. Whether on a boat in the middle of nowhere or in remote regions, WikiMed is your perfect companion.

Winlink Global Radio Email (https://winlink.org/) is a worldwide messaging system that enables licensed amateur radio operators and authorized government users to send and receive email with attachments over radio frequencies, independent of the internet. It functions as a store-and-forward network using smart radio relays to bridge gaps where traditional communication infrastructure fails, making it a critical tool for emergency and disaster relief communications.

Wire (https://wire.com/en/) is an end-to-end encrypted communication and collaboration platform developed by Wire Swiss GmbH, designed for both personal use and secure business collaboration. It supports text messaging, voice calls, video conferences, file sharing, and guest rooms for external partners, available on iOS, Android, Windows, macOS, Linux, and via web browsers.

WSJT-X (https://wsjt.sourceforge.io/wsjtx.html) is an open-source computer program designed to facilitate amateur radio communication using very weak signals, developed originally by Joe Taylor (K1JT) and now maintained by a core team of contributors including Uwe Risse (DG2YCB) and Roger Rehr (W3SZ). The software implements multiple digital protocols, including FT8, FT4, JT65, JT9, WSPR, and Echo, which enable reliable contacts under extreme weak-signal conditions, EME (moonbounce), meteor scatter, and propagation path probing. These modes use specialized digital signal processing (DSP) techniques to decode signals as low as -31 dB in a 2500 Hz bandwidth, often with only a few watts of power and modest antennas.

YAAC (Yet Another APRS Client) (https://www.ka2ddo.org/ka2ddo/YAAC.html) is a platform-independent Java application designed for monitoring and contributing to the Automatic Packet Reporting System (APRS) network. Developed by Andrew Pavlin (KA2DDO), it functions as a stand-alone client, an I-Gate (RF-Internet gateway), or an AX.25 digipeater. The software is open-source under the GNU Lesser General Public License and uses OpenStreetMap data to render real-time tactical maps for tracking assets without requiring internet connectivity.

Zello (https://zello.com/) is a live voice push-to-talk (PTT) communication platform that transforms smartphones, tablets, and computers into digital two-way radios using Wi-Fi or cellular networks. Developed by the Austin, Texas-based company Zello Inc., the app allows users to communicate instantly with one or many people in unlimited secure, private channels without traditional phone calls or text messages.

ZeroNet (https://zeronet.io/) is a decentralized web-like network of peer-to-peer users, created by Tamas Kocsis in 2015. The programming for the network was based in Budapest, Hungary. It is built in Python and fully open source. Instead of having an IP address, sites are identified by a public key (specifically a bitcoin address). The private key allows the owner of a site to sign and publish changes, which propagate through the network. Sites can be accessed through an ordinary web browser when using the ZeroNet application, which acts as a local webhost for such pages. In addition to using bitcoin cryptography, ZeroNet uses trackers from the BitTorrent network to negotiate connections between peers. ZeroNet is not anonymous by default, but it supports routing traffic through the Tor network.

Zim (https://zim-wiki.org/) is a graphical text editor used to maintain a collection of wiki pages. Each page can contain links to other pages, simple formatting and images. Pages are stored in a folder structure, like in an outliner, and can have attachments. Creating a new page is as easy as linking to a nonexistent page. All data is stored in plain text files with wiki formatting. Various plugins provide additional functionality, like a task list manager, an equation editor, a tray icon, and support for version control.

Dark Web Email Providers (Access with the TOR Browser)

(Updated and confirmed working on 28 March 2026)

Cock.li (NSFW) –
rurcblzhmdk22kttfkel2zduhyu3r6to7knyc7wiorzrx5gw4c3lftad.onion

Mail2Tor –
mail2torjgmxgexntbrmhvgluavhj7ouul5yar6ylbvjkxwqf6ixkwyd.onion

ProtonMail –
protonmailrmez3lotccipshtkleegetolb73fuirgj7r4o4vfu7ozyd.onion

RiseUp – 3xeiol2bnhrsqhcsaifwtnlqkylrerdspzua7bcjrh26qlrrrctfobid.onion

Torbox –
torbox36ijlcevujx7mjb4oiusvwgvmue7jfn2cvutwa6kl6to3uyqad.onion

OnionMail –
pflujznptk5lmuf6xwadfqy6nffykdvahfbljh7liljailjbxrgvhfid.onion

Systemli.org –
7sk2kov2xwx6cbc32phynrifegg6pklmzs7luwcggtzrnlsolxxuyfyd.onion

SecretMail –
2nxpboa3ya52j5au4gxwkdt4nxoh5g4y4f3tuqedlza46y35jmv6doid.onion

Hidden Mail Onion Server –
5nm4mdhzyfbif6i5qv3kh4i7j2trlbuvujsencsqn55opaa3d6qhfcqd.onion

Dozaru Onion Mail Server –
eot3almpracnkz7gz3r5yr3qaymngqsrmvbica2shw5zuc52az2gxoqd.onion

Morke –
6n5nbusxgyw46juqo3nt5v4zuivdbc7mzm74wlhg7arggetaui4yp4id.onion

CS.Email (Disposable Temporarily Email) –
csmail3thcskmzvjicww3qdkvrhb6pb5s7zjqtb3gdst6guby2stsiqd.onion
(Receive Only)

Adunanza Onion Mail –
j3bv7g27oramhbxxuv6gl3dcyfmf44qnvju3offdyrap7hurfprq74qd.onion

Systemli –
2nxpboa3ya52j5au4gxwkdt4nxoh5g4y4f3tuqedlza46y35jmv6doid.onion

Underworld.dog Onion Email –
fozdean5ayswi6jtseg2fgyysqt3dskoosmoc6gnqia4dxwxiuvg3oad.onion

And a few other sites to help you navigate the Dark Web…

Dark Search -
http://darkzqtmbdeauwq5mzcmgeeuhet42fhfjj4p5wbak3ofx2yqgecoeqyd.onion/

Dark Web Link -
http://dwltorbltw3tdjskxn23j2mwz2f4q25j4ninl5bdvttiy4xb6cqzikid.onion/

OnionFind: A useful dark web search engine that allows you to search incredibly detailed queries. -
http://ofinde3b67voi7xiq3qflof2mwriwngicd7glwvf3bclgdgcjfozlzqd.onion/

Tenebris [The Dark Net of Reddit] This is a decentralized forum on the dark web where you can ask any question you like without getting censored. -
http://tenebrispoyfrcup4k24lciwrh4gc5735hmld4dweq7his7zh423opqd.onion/

The Safe Onion Links -
http://forumup4mrybxqweysxevr3nfivmphrwq5tngxbhixwppzji34y454id.onion/

ZeroBin is a way to share the content you get from dark web resources. It is a reliable messaging tool where you copy/paste a text or image and send it to your addressee.
http://zerobinftagjpeeebbvyzjcqyjpmjvynj5qlexwyxe7l3vqejxnqv5qd.onion/

Finis Libri